PAT-NO: JP02000076139A

DOCUMENT-IDENTIFIER: JP 2000076139 A

TITLE: PORTABLE INFORMATION STORAGE MEDIUM

PUBN-DATE: March 14, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
TANNO, MASAAKI	N/A
TAKEDA, TADAO	N/A
BAN, KOJI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NIPPON TELEGR & TELEPH CORP <NTT>	N/A

APPL-NO: JP10243380

APPL-DATE: August 28, 1998

INT-CL (IPC): G06F012/14, G06K019/073

ABSTRACT:

PROBLEM TO BE SOLVED: To erase secret information and to preserve required information upon detecting a physical attack from the outside.

SOLUTION: A sensor element 2 detects the physical attack from the outside. A first memory element 3 is a writable/readable memory and a second memory element 5 is a read-only memory capable of white only once. A voltage monitoring means 8 monitors the output voltage of a battery 7. When the physical attack is detected by the sensor element 2 or when the output voltage

abnormality of the battery 7 is detected by a voltage monitoring mechanism 8, a memory control mechanism 6 reads information to be preserved from the memory element 3, writes it in the memory element 5 and erases the secret information stored in the memory element 3.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to the technology which defends important storage information from an unjust attack while checking analyzing storage information, such as an IC card, unjustly in detail about the security of the portable small information-storage medium represented by the IC card.
[0002]
[Description of the Prior Art] In order to protect storage information from the physical attack unjust as an information-storage medium which memorizes extra sensitive information etc. conventionally, what builds in a physical security mechanism is proposed. as a typical example, there is muABYSS (bibliography: -- S.H.Weigart, "Physical security for the mu ABYSS system", and Proc.1987 IEEE Symp.onSecurity and Privacy, Oakland, CA, pp.52-58 and April 1987) o U.S. IBM
[0003] This muABYSS cannot observe the interior of a module, unless the whole module is wrapped in the metal thin line in the shape of a cocoon and a metal thin line is cut. When a metal thin line is cut, the security mechanism built in the module detects resistance change of a metal thin line, and eliminates extra sensitive information immediately. Disclosure of extra sensitive information is prevented by this. Sensing of the attack from the outside of the information-storage medium which contains other security mechanisms is performing operation which eliminates important information.
[0004]
[Problem(s) to be Solved by the Invention] As mentioned above, it becomes impossible to read extra sensitive information with being natural even if the security mechanism of the conventional information-storage medium performs regular information read-out operation to an information-storage medium after a security mechanism detects an attack, in order to prevent the disclosure by eliminating extra sensitive information. Since the balance data in a card would be eliminated if a security mechanism operates according to intentionally, negligence, or accident when the carried type information-storage medium which contained such a security mechanism is applied to a prepaid card or a cybermoney card, there was a trouble that monetary value of a card could not be restored. Moreover, the built-in cell was exhausted and there was also a trouble that indispensable data were lost. Such a problem will not have the basis of the balance data fed into a new prepaid card in case the prepaid card damaged according to a cell piece, accident, etc. is exchanged at the window, and any of a card employment company and a user they are will suffer money-damage. this invention aims at offering the carried type information-storage medium which can save required information while it eliminates extra sensitive information, when it is made in order to solve the above-mentioned technical problem, and th physical attack from the outside is detected. Moreover, when the attack on a built-in cell and exhaustion of a cell are detected, while eliminating extra sensitive information, it aims at offering the carried type information-storage medium which can save required information.
[0005]
[Means for Solving the Problem] The carried type information-storage medium of this invention The sensor element according to claim 1 which detects the physical attack from the outside like (2), The 1st memory device (3) in which write-in read-out is possible, and the 2nd memory device only for read-out which can be written in only at once (5), It has the memory control means (6) interlocked with the response of a sensor element. the above-mentioned memory control means When a physical attack is detected by the sensor element, while reading the information which should b saved from the 1st memory device and writing in the 2nd memory device, the extra sensitive information memorized b the 1st memory device is eliminated. Thus, since memory control means eliminate the extra sensitive information memorized by the 1st memory device while they read the information which should be saved from the 1st memory

device and write it in the 2nd memory device, when a physical attack is detected by the sensor element, they can reconcile prevention of leakage of secrets and preservation of required information. Moreover, it has a voltage surveillance means (8) according to claim 2 to supervise the output voltage of the cell for electric power supplies (7), and this cell like, and the above-mentioned memory control means eliminate the extra sensitive information memorized by the 1st memory device while they read the information which should be saved from the 1st memory device and writ it in the 2nd memory device, when the abnormalities in output voltage of a cell are detected by the voltage surveillance means. Thus, since memory control means eliminate the extra sensitive information memorized by the 1st memory device while they read the information which should be saved from the 1st memory device and write it in the 2nd memory device, when voltage change which originates in the attack [exhausting / with time / a cell] to a cell by the voltage surveillance means is detected, they can reconcile prevention of leakage of secrets and preservation of required information.

[0006]

[Embodiments of the Invention] Next, the gestalt of operation of this invention is explained in detail with reference to a drawing. Drawing 1 is the block diagram showing the composition of the carried type information-storage medium use as the gestalt of operation of this invention. The sensor element 2 as which the carried type information-storage mediun 1 of the gestalt of this operation detects the physical attack from the outside, The 1st memory device 3 in which write-i read-out is possible, and the external ON appearance carport 4 for considering an exchange of data as external reader/writer, When a physical attack is detected by the 2nd memory device 5 and sensor element 2 only for read-out which can be written in only at once, Or when the abnormalities in output voltage of a cell are detected by the voltage surveillance mentioned later, while reading the information which should be saved from the 1st memory device 3 and writing in the 2nd memory device 5 It has the memory controlling mechanism 6 which eliminates the extra sensitive information memorized by the 1st memory device 3, the cell 7 for supplying power to the 1st, the 2nd memory device 3 and 5, and memory controlling mechanism 6 grade, and the voltage surveillance 8 which supervises the output voltage of a cell 7.

[0007] The sensor element 2 is a sensor which detects the physical attack (physical stimulus it is considered that are unjust actions, such as opening of a sealing agent) from the outside, and is constituted by the electronic circuitry which detects the change more than the electric resistance of the photo detector which detects the incident light to the interior by the sealing agent of a medium 1 having been opened, and a closure portion, or the specified quantity of electrostatic capacity, or the shock sensor which detects the shock more than the specified quantity. The electronic circuitry which detects change of the electric resistance of a closure portion measures the electric resistance of a metal plate establishec so that the composition of drawing 1 might be optically covered in a sealing agent, and detects change of the electric resistance by the metal plate having been removed by the attack from the outside. The electronic circuitry which detect change of the electrostatic capacity of a closure portion measures the electrostatic capacity between the above-mentioned metal plates which counter on both sides of a sealing agent, and detects change of the electrostatic capacity by the metal plate having been removed by the attack from the outside.

[0008] The 1st memory device 3 is memory used as work memory for temporary storage, and is constituted by non-volatile memory, such as volatile memory, such as RAM (Random Access Memory), or EEPROM (Electrically Erasable and Programmable Read Only Memory), while it memorizes extra sensitive information, such as a code key, individual authentication information and the balance, and a savings point size.

[0009] Only at once, the 2nd memory device 5 is the non-volatile memory which can be written in electrically, and is constituted by the one time PROM (Programmable Read Only Memory). A fuse is prepared in this one time PROM fo every memory cell, and there is a fuse fusing type which melts a fuse in the case of data writing in it. In addition, the 2nd memory device 5 is carried in a medium 1 still in the state in the state where it does not write in.

[0010] As a memory controlling mechanism 6, you may use central processing units (CPU), such as a memory management unit (MMU) of a computer, and a microprocessor, for example. Next, operation when the carried type information-storage medium 1 of the gestalt of this operation receives the attack from the outside is explained. Drawin 2 is the flow chart view showing operation at the time of a medium 1 receiving an attack.

[0011] When a physical attack is detected by the sensor element 2, or when the abnormalities in output voltage of a cel 7 are detected by the voltage surveillance 8 (drawing 2 step 101), the memory controlling mechanism 6 reads the information which should be saved [point size / savings / the balance,] from the storage region of the extra sensitive information in the 1st memory device 3, and writes the read information in the 2nd memory device 5 (Step 102). Then, the memory controlling mechanism 6 eliminates extra sensitive information by rewriting to the storage region of the extra sensitive information in the 1st memory device 3 (Step 103).

[0012] As mentioned above, by the carried type information-storage medium 1 of the gestalt of this operation, since

extra sensitive information is eliminated when a physical attack is detected, or when the abnormalities in output voltage of the cell 7 by exhausting [a cell 7 / exhausting / removal or] are detected, decode of extra sensitive information can be made impossible. Moreover, about the information among extra sensitive information to be saved, the memory controlling mechanism 6 writes in the 2nd memory device 5.

[0013] For example, when the carried type information-storage medium of this invention is applied to a prepaid card, a cybermoney card, or a point card, after deleting extra sensitive information, such as a code key and individual authentication information, from the memory device 3 in a card and writing in a memory device 5 about balance data o: a savings point size, it deletes from a storage region from the first. Even when a security mechanism can operate, disclosure of extra sensitive information can be prevented, when an attack is intentionally added to a card, and a securit mechanism operates according to accidental accident by this, it becomes possible to save information, such as the balance.

[0014] Therefore, if the prepaid card of balance zero is destroyed intentionally, since it is recorded on the 2nd memory device 5 of this card that the balance is zero and the information on the memory device 5 which can moreover be writte in only at once cannot be rewritten, it can prevent those who destroyed the card of balance zero intentionally reporting themselves as the card became poor, and converting into money unlawfully. Moreover, it can be checked whether since the writing to the 2nd memory device 5 was performed when the card was opened, when checking the write-in state of the 2nd memory device 5, the attack has been added to a card. Therefore, it becomes possible to judge whether it is the card which suffered damage though the card was closed and the normal card was pretended after opening a card unjustly.

[0015] In addition, the capacitor which is not illustrated is arranged in parallel by the cell 7, and drawing 2 can be operated even when a cell 7 is removed by the charge stored in this capacitor. Moreover, the carried type information-storage medium 1 of this invention may be the gestalt of the IC card which embedded the semiconductor chip on the card made of a resin, and may be the gestalt of PCMCIA (PC card) which built thin shape parts into the thin shape case Moreover, the composition which could constitute the sensor element 2, memory devices 3 and 5, the memory controlling mechanism 6, and the voltage surveillance 8 from independent parts, and was accumulated on one chip may be used.

[0016]

[Effect of the Invention] According to this invention, the unjust attack and the accidental accident from the outside, exhaustion of a built-in cell, etc. are interlocked with by preparing a sensor element, the 1st memory device, the 2nd memory device, and memory control means in claims 1 and 2 like a publication, and since elimination of extra sensitiv information and the information which should be saved are held, prevention of leakage of secrets and preservation of required information can be reconciled. If this carrying type information-storage medium is unjustly opened for analys: of operation or decode of storage information, since extra sensitive information will be eliminated immediately, the format of an encryption procedure, a code key, and a storage region etc. can protect information important for decode from disclosure. Since the extra sensitive information currently written in the 1st memory device though the informatic written in the 2nd memory device was decoded is eliminated, it becomes impossible to restore original extra sensitive information. If the carried type information-storage medium it became impossible to use by exhaustion of accidental accident and a built-in cell is brought to the management engine of service when this carrying type information-storage medium is applied to a prepaid card or a point card, information required for a new carried type information-storage medium can be copied. Moreover, it can judge whether it is the medium which suffered damage by checking the write-in state of the 2nd memory device, though it recloses after those who destroyed the carried type information-storage medium of balance zero intentionally can also cope with the crime of reporting oneself as the medium became poor, ar requiring illegal liquidation and open a carried type information-storage medium unjustly, and a normal medium is pretended.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－76139
（P2000－76139A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｄ	５Ｂ０１７
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	５Ｂ０３５

審査請求　未請求　請求項の数２　ＯＬ　（全５頁）

(21)出願番号　特願平10－243380

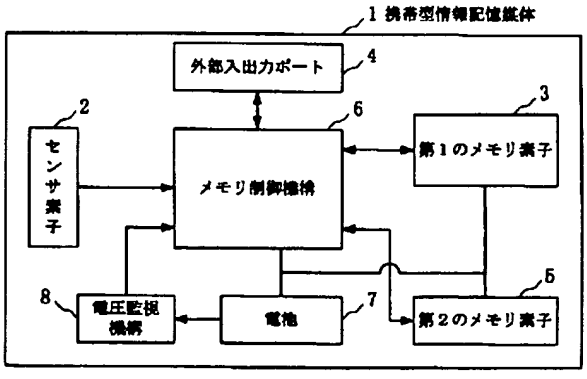
(22)出願日　平成10年８月28日(1998.8.28)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　丹野　雅明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　竹田　忠雄
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100064621
弁理士　山川　政樹

最終頁に続く

(54)【発明の名称】　携帯型情報記憶媒体

(57)【要約】
【課題】　外部からの物理的な攻撃を検知したとき、機密情報を消去すると共に必要な情報を保存する。
【解決手段】　センサ素子２は外部からの物理的な攻撃を検知する。第１のメモリ素子３は書き込み読み出し可能なメモリで、第２のメモリ素子５は一度だけ書き込み可能な読み出し専用のメモリである。電圧監視手段８は電池７の出力電圧を監視する。メモリ制御機構６は、センサ素子２によって物理的な攻撃が検知されたとき、あるいは電圧監視機構８によって電池７の出力電圧異常が検知されたとき、メモリ素子３から保存すべき情報を読み出してメモリ素子５に書き込むと共に、メモリ素子３に記憶された機密情報を消去する。



【特許請求の範囲】
【請求項１】　外部からの物理的な攻撃を検知するセンサ素子と、
書き込み読み出し可能な第１のメモリ素子と、
一度だけ書き込み可能な読み出し専用の第２のメモリ素子と、
センサ素子の応答に連動するメモリ制御手段とを有し、前記メモリ制御手段は、センサ素子によって物理的な攻撃が検知されたとき、第１のメモリ素子から保存すべき情報を読み出して第２のメモリ素子に書き込むと共に、第１のメモリ素子に記憶された機密情報を消去することを特徴とする携帯型情報記憶媒体。
【請求項２】　請求項１記載の携帯型情報記憶媒体において、
電力供給用の電池と、
この電池の出力電圧を監視する電圧監視手段とを有し、前記メモリ制御手段は、電圧監視手段によって電池の出力電圧異常が検知されたとき、第１のメモリ素子から保存すべき情報を読み出して第２のメモリ素子に書き込むと共に、第１のメモリ素子に記憶された機密情報を消去することを特徴とする携帯型情報記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカードに代表される携帯可能な小型情報記憶媒体のセキュリティに関し、詳しくはＩＣカード等の記憶情報を不正に解析することを阻害すると共に、重要な記憶情報を不正な攻撃から防御する技術に関するものである。
【０００２】
【従来の技術】従来より、機密情報等を記憶する情報記憶媒体として、不正な物理的攻撃から記憶情報を守るために、物理的なセキュリティ機構を内蔵するものが提案されている。代表的な例として、米国ＩＢＭ社のμＡＢＹＳＳ（参考文献：S.H.Weigart,"Physical security for the μＡＢＹＳＳ system",Proc.1987 IEEE Symp.on Security and Privacy,Oakland,CA,pp.52-58,April 1987）がある。
【０００３】このμＡＢＹＳＳは、モジュール全体が金属細線で繭状に包まれており、金属細線を切断しない限り、モジュール内部を観測することができない。金属細線が切断された場合、モジュールに内蔵されたセキュリティ機構が金属細線の抵抗変化を検知し、即座に機密情報を消去する。これによって機密情報の漏洩を防止するものである。このほかのセキュリティ機構を内蔵する情報記憶媒体も外部からの攻撃を感知すると重要な情報を消去する動作を行っている。
【０００４】
【発明が解決しようとする課題】以上のように、従来の情報記憶媒体のセキュリティ機構は、機密情報を消去することによってその漏洩を防止するため、セキュリティ機構が攻撃を検知した後は、情報記憶媒体に対し正規の情報読み出し操作を行っても、当然の事ながら機密情報を読み出すことは不可能となる。このようなセキュリティ機構を内蔵した携帯型情報記憶媒体をプリペイドカードや電子マネーカードに適用した場合、故意、過失あるいは事故によってセキュリティ機構が動作すると、カード内の残額データが消去されるため、カードの貨幣価値を復元できないという問題点があった。また、内蔵電池が消耗し、必須のデータが失われるという問題点もあった。このような問題は、電池切れや事故等により破損したプリペイドカードを、窓口で交換する際、新しいプリペイドカードに投入する残高データの根拠がないことになり、カード運用会社と利用者の何れかが金銭的被害を被ることとなる。本発明は、上記課題を解決するためになされたもので、外部からの物理的な攻撃を検知したとき、機密情報を消去すると共に必要な情報を保存することができる携帯型情報記憶媒体を提供することを目的とする。また、内蔵電池に対する攻撃や電池の消耗を検知したとき、機密情報を消去すると共に必要な情報を保存することができる携帯型情報記憶媒体を提供することを目的とする。
【０００５】
【課題を解決するための手段】本発明の携帯型情報記憶媒体は、請求項１に記載のように、外部からの物理的な攻撃を検知するセンサ素子（２）と、書き込み読み出し可能な第１のメモリ素子（３）と、一度だけ書き込み可能な読み出し専用の第２のメモリ素子（５）と、センサ素子の応答に連動するメモリ制御手段（６）とを有し、上記メモリ制御手段は、センサ素子によって物理的な攻撃が検知されたとき、第１のメモリ素子から保存すべき情報を読み出して第２のメモリ素子に書き込むと共に、第１のメモリ素子に記憶された機密情報を消去するものである。このように、メモリ制御手段は、センサ素子によって物理的な攻撃が検知されたとき、第１のメモリ素子から保存すべき情報を読み出して第２のメモリ素子に書き込むと共に、第１のメモリ素子に記憶された機密情報を消去するので、機密漏洩の防止と必要な情報の保存を両立させることができる。また、請求項２に記載のように、電力供給用の電池（７）と、この電池の出力電圧を監視する電圧監視手段（８）とを有し、上記メモリ制御手段は、電圧監視手段によって電池の出力電圧異常が検知されたとき、第１のメモリ素子から保存すべき情報を読み出して第２のメモリ素子に書き込むと共に、第１のメモリ素子に記憶された機密情報を消去するものである。このように、メモリ制御手段は、電圧監視手段によって電池の経時的な消耗や電池への攻撃に起因する電圧変化が検知されたとき、第１のメモリ素子から保存すべき情報を読み出して第２のメモリ素子に書き込むと共に、第１のメモリ素子に記憶された機密情報を消去するので、機密漏洩の防止と必要な情報の保存を両立させる

ことができる。

【0006】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。図1は本発明の実施の形態となる携帯型情報記憶媒体の構成を示すブロック図である。本実施の形態の携帯型情報記憶媒体1は、外部からの物理的な攻撃を検知するセンサ素子2と、書き込み読み出し可能な第1のメモリ素子3と、外部のリーダ／ライタ等とデータのやり取りをするための外部入出力ポート4と、一度だけ書き込み可能な読み出し専用の第2のメモリ素子5と、センサ素子2によって物理的な攻撃が検知されたとき、あるいは後述する電圧監視機構によって電池の出力電圧異常が検知されたとき、第1のメモリ素子3から保存すべき情報を読み出して第2のメモリ素子5に書き込むと共に、第1のメモリ素子3に記憶された機密情報を消去するメモリ制御機構6と、第1、第2のメモリ素子3，5、メモリ制御機構6等に電力を供給するための電池7と、電池7の出力電圧を監視する電圧監視機構8とを有している。

【0007】センサ素子2は、外部からの物理的な攻撃（封止材の開封などの不正な行為と見なされる物理的な刺激）を検知するセンサであり、媒体1の封止材が開封されたことによる内部への入射光を検知する受光素子、封止部分の電気抵抗若しくは静電容量の所定量以上の変化を検知する電子回路、あるいは所定量以上の衝撃を検知する衝撃センサ等によって構成される。封止部分の電気抵抗の変化を検知する電子回路は、封止材内に図1の構成を光学的に遮蔽するように設けられた金属板の電気抵抗を測定するものであり、外部からの攻撃によって金属板が取り外されたことによる電気抵抗の変化を検知するものである。封止部分の静電容量の変化を検知する電子回路は、封止材を挟んで対向する上記金属板との間の静電容量を測定するものであり、外部からの攻撃によって金属板が取り外されたことによる静電容量の変化を検知するものである。

【0008】第1のメモリ素子3は、暗号キーや個人認証情報、残金や積立ポイント数等の機密情報を記憶すると共に、一時記憶用のワークメモリとして使用されるメモリであり、ＲＡＭ（Random Access Memory）等の揮発性メモリあるいはＥＥＰＲＯＭ（Electrically Erasable and Programmable Read Only Memory ）等の不揮発性メモリによって構成される。

【0009】第2のメモリ素子5は、一度だけ電気的に書き込み可能な不揮発性メモリであり、ワンタイムＰＲＯＭ（Programmable Read Only Memory ）によって構成される。このワンタイムＰＲＯＭには、メモリセル毎にヒューズを設け、データ書き込みの際にヒューズを溶断するヒューズ溶断型等がある。なお、第2のメモリ素子5は、未書込状態のまま媒体1に搭載される。

【0010】メモリ制御機構6としては、例えばコンピュータのメモリマネージメントユニット（ＭＭＵ）やマイクロプロセッサ等の中央処理装置（ＣＰＵ）を用いてもよい。次に、本実施の形態の携帯型情報記憶媒体1が外部からの攻撃を受けた場合の動作を説明する。図2は媒体1が攻撃を受けた際の動作を示すフローチャート図である。

【0011】センサ素子2によって物理的な攻撃が検知されたとき、あるいは電圧監視機構8によって電池7の出力電圧異常が検知されたとき（図2ステップ101）、メモリ制御機構6は、第1のメモリ素子3内にある機密情報の記憶領域から残金や積立ポイント数等の保存すべき情報を読み出し、読み出した情報を第2のメモリ素子5に書き込む（ステップ102）。続いて、メモリ制御機構6は、第1のメモリ素子3内にある機密情報の記憶領域に対して、書き換えを行うことにより、機密情報を消去する（ステップ103）。

【0012】以上のように、本実施の形態の携帯型情報記憶媒体1では、物理的な攻撃が検知されたとき、あるいは電池7の取り外し若しくは消耗による電池7の出力電圧異常が検知されたとき、機密情報を消去するので、機密情報の解読を不可能にすることができる。また、機密情報のうち、保存が必要な情報に関しては、メモリ制御機構6が第2のメモリ素子5に書き込む。

【0013】例えば、プリペイドカードや電子マネーカードあるいはポイントカードに本発明の携帯型情報記憶媒体を適用する場合、暗号キーや個人認証情報等の機密情報をカード内のメモリ素子3から抹消し、残高データや積立ポイント数についてはメモリ素子5に書き込んだ上で、元々の記憶領域から抹消する。これにより、カードに対して故意に攻撃が加えられた場合には、セキュリティ機構が動作して機密情報の漏洩を防ぐことができ、偶発的な事故によってセキュリティ機構が動作した場合でも、残金等の情報を保存することが可能となる。

【0014】したがって、残金零のプリペイドカードを故意に破壊すると、このカードの第2のメモリ素子5に残金が零であることが記録され、しかも一度だけ書き込みが可能なメモリ素子5の情報を書き換えることはできないので、残金零のカードを故意に破壊した者が、カードが不良になったと申告して不法に換金することを防ぐことができる。また、カードを開封すると、第2のメモリ素子5への書き込みが行われるので、第2のメモリ素子5の書込状態を確認すれば、カードに対して攻撃が加えられたか否かを確認することができる。よって、カードを不正に開封した後に、カードを封止して正常なカードを装ったとしても、被害を受けたカードであるか否かを判断することが可能となる。

【0015】なお、電池7には図示しないコンデンサが並列に配設されており、このコンデンサに蓄えられた電荷により、電池7が取り外された場合でも、図2の動作を行えるようになっている。また、本発明の携帯型情報

記憶媒体1は、樹脂製のカードに半導体チップを埋め込んだＩＣカードの形態であってもよいし、薄型部品を薄型ケースに組み込んだＰＣＭＣＩＡ（ＰＣカード）の形態であってもよい。また、センサ素子２、メモリ素子３，５、メモリ制御機構６、電圧監視機構８を独立した部品で構成してもよいし、１チップに集積した構成でもよい。

【００１６】

【発明の効果】本発明によれば、請求項１，２に記載のように、センサ素子、第１のメモリ素子、第２のメモリ素子及びメモリ制御手段を設けることにより、外部からの不正な攻撃や偶発的な事故や内蔵電池の消耗等に連動して、機密情報の消去と保存すべき情報の保持を行うため、機密漏洩の防止と必要な情報の保存を両立させることができる。動作解析や記憶情報の解読のために、本携帯型情報記憶媒体を不正に開封すると、即座に機密情報が消去されるため、暗号化手順、暗号キー、記憶領域のフォーマット等、解読に重要な情報を漏洩から守ることができる。仮に、第２のメモリ素子に書き込んだ情報が解読されたとしても、第１のメモリ素子に書き込まれていた機密情報が消去されているので、本来の機密情報を復元することは不可能となる。本携帯型情報記憶媒体をプリペイドカードやポイントカードに適用した場合、偶発的な事故や内蔵電池の消耗により使用できなくなった携帯型情報記憶媒体をサービスの運営機関に持参すれば、新しい携帯型情報記憶媒体に必要な情報をコピーすることができる。また、残金零の携帯型情報記憶媒体を故意に破壊した者が、媒体が不良になったと申告して不法な換金を要求する犯罪にも対処でき、携帯型情報記憶媒体を不正に開封した後に封止し直して正常な媒体を装ったとしても、第２のメモリ素子の書込状態を確認することで、被害を受けた媒体であるか否かを判断することができる。

【図面の簡単な説明】

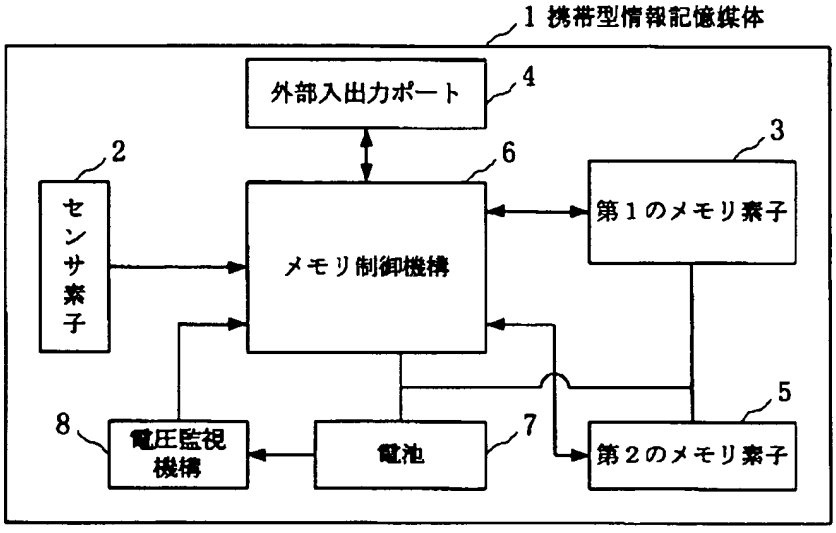
【図１】　本発明の実施の形態となる携帯型情報記憶媒体の構成を示すブロック図である。

【図２】　図１の携帯型情報記憶媒体が攻撃を受けた際の動作を示すフローチャート図である。

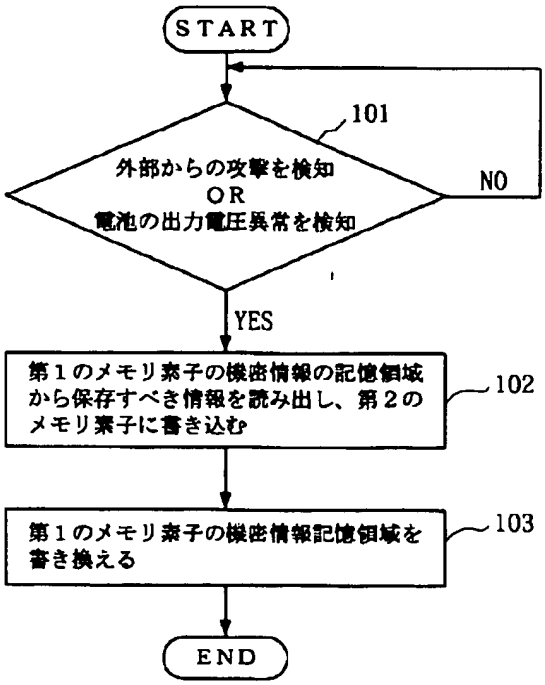
【符号の説明】

１…携帯型情報記憶媒体、２…センサ素子、３…第１のメモリ素子、４…外部入出力ポート、５…第２のメモリ素子、６…メモリ制御機構、７…電池、８…電圧監視機構。

【図１】



【図2】



フロントページの続き

(72)発明者　伴　弘司
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

Fターム(参考)　5B017 AA03 AA08 BA08 CA14
5B035 AA15 BB09 CA38